IMPLEMENTASI ALGORITMA *RSA* UNTUK PENGAMANAN DATA BERBENTUK TEKS

Pahrizal[1], David Pratama[2]

[1,2]Informatika, Fakultas Teknik, Universitas Muhammadiyah Bengkulu
Jl. Bali Po. Box, 118 Kota Bengkulu 38119 INDONESIA
(telp : 0736-22765; fax : 0736-26161)

[1]fahrizal1202@gmail.com
[2]d_vidpratama@gmail.com

Abstrak : Perkembangan Teknologi Informasi telah menyebabkan perubahan dan cara pandang hidup manusia maupun suatu organisasi. Perkembangan yang sedemikian cepatnya membawa dunia memasuki era baru yang lebih cepat dari yang pernah dibayangkan sebelumnya. Saat ini, keamanan terhadap data yang tersimpan dalam *file* sudah menjadi persyaratan mutlak. Pengamanan terhadap *file* yang terhubung dengan komputer sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh "orang dalam" atau pihak–pihak yang langsung berhubungan dengan *file* tersebut. Tujuan penelitian untuk menerapkan keamanan *file* menggunakan Algoritma *RSA*. Aplikasi ini mempunyai dua teknik pembacaan yaitu teknik enkripsi (mengubah *file* asli menjadi *file* yang tidak dapat dibaca) dan dekripsi (mengubah *file* yang tidak dapat dibaca menjadi *file* asli). Aplikasi ini menggunakan algoritma *RSA* yang merupakan *block cipher*, dimana sebuah *plaintext* dan *ciphertext* merupakan integer antara 0 dan n-1.
Kata Kunci : Keamanan, Aplikasi, Teknik, *RSA*

Abstract: The development of information technology has changed the way of life and humans as well as an organization. Developments so quickly brings the world enters a new era faster than ever imagined before. Nowadays, security of data stored in the file has become an absolute requirement. Security of files connected to the computer is no longer guarantee the security of the data because the data leaks can be caused by an "insider" or parties directly associated with the file. The research objective is to implement file security using RSA algorithm. This application has two reading techniques that encryption techniques (changing the original file into a file that can not be read) and decryption (modify files that can not be read into the original file). This application uses an RSA algorithm is a block cipher, where a plaintext and ciphertext is an integer between 0 and n-1.
Keywords: Security, Application, Engineering, RSA

I. PENDAHULUAN

Teknologi Informasi telah menyebabkan perubahan dan cara pandang hidup manusia maupun suatu organisasi. Perkembangan yang sedemikian cepatnya membawa dunia memasuki era baru yang lebih cepat dari yang pernah dibayangkan sebelumnya. Seperti komputer yang tidak hanya berfungsi sebagai alat pengolahan data saja, namun telah menjadi senjata utama dalam berkompetisi. Hal ini dikarenakan dengan adanya komputer dapat mempermudah dan mempercepat suatu pekerjaan dalam mengakses informasi.

Berbagai organisasi, perusahaan, atau pun pihak–pihak lain telah memanfaatkan teknologi basis data untuk menyimpan dan mengelola data organisasi atau perusahaannya. Untuk menghindari hal itu terjadi, maka dibutuhkan sebuah metode penyandian, ilmu sekaligus seni guna menjaga *file* yang disebut juga dengan kriptografi. Salah satu perangkat lunak kriptografi adalah *Pretty Good Privacy (PGP)* yang juga bisa

digunakan secara *online* maupun *offline*. Selain dapat mengamankan *file*, perangkat lunak ini juga dapat memberikan tanda tangan digital (*digital signature*) yang mampu memenuhi tiga aspek keamanan yaitu integritas data, otentikasi, dan nirpenyangkalan.

Berdasarkan latar belakang diatas penulis bermaksud mengajukan judul penelitian yang berjudul "Implementasi Algoritma RSA Untuk Pengamanan Data Berbentuk Teks**".**

II. LANDASAN TEORI

2.1 Kriptografi RSA

Pada tahun 1977, Ronald L. Rivest, Adi Shamir, dan Leonard M. Adleman merumuskan algoritma praktis yang mengimplementasikan sistem kriptografi kunci publik yang disebut dengan sistem kriptografi RSA. Sepasang kunci yang dipakai pada kedua proses ini adalah kunci publik (*e,n*) sebagai kunci enkripsi dan kunci privat *d* sebagai sebagai kunci dekripsi dimana *e*, *d* dan *n* adalah bilangan bulat positif. Algoritma RSA adalah sebuah *block cipher algorithm* (algoritma yang bekerja per blok data) yang mengelompokkan plaintext menjadi blok-blok terlebih dahulu sebelum dilakukan enkripsi hingga menjadi ciphertext [1].

Untuk menentukan algoritma Kriptografi yang akan digunakan dalam sistem keamanan data selain pertimbangan kekuatan terhadap serangan Cryptanalis dan *Bruteforce* yang tidak kalah penting adalah pertimbangan kecepatan. Pada saat ini terdapat berbagai macam algoritma Kriptografi simetri maupun asimetri. Jika suatu algoritma Kriptografi dipercaya kuat namun diketahui lamba dalam proses penyandiannya maka tidak akan dijadikan pilihan oleh pengguna. Pertimbangan kecepatan ini akan menjadi lebih diutamakan lagi jika pemakaian algoritma Kriptografi menyangkut jaringan komputer terutama pada arsitektur clien-server [2].

2.2 *Algoritma RSA*

Dalam kriptografi, RSA adalah algoritma untuk enkripsi kunci publik (p*ublic-key encryption*). Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (*signing*) dan untuk enkripsi (*encryption*) dan salah satu penemuan besar pertama dalam kriptografi kunci publik. RSA masih digunakan secara luas dalam protokol-protokol perdagangan elektronik, dan dipercayai sangat aman karena diberikan kunci-kunci yang cukup panjang dan penerapan-penerapannya yang sangat *up-to-date* (mutakhir) [3].

Pertama-tama, *plaintext* dienkripsi menjadi blok-blok, dimana setiap blok memiliki bilangan biner kurang dari n untuk n suatu nilai. Dengan begitu jadi ukuran blok harus kurang dari atau sama dengan log2(n). Enkripsi dan dekripsi dari suatu blok plaintext M dan blok *ciphertext* C:

- $C = M^e \bmod n$
- $M = Cd \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Untuk mendapatkan hal di atas syarat-syarat yang harus dipenuhi adalah sebagai berikut:

1. Nilai e, d, n dapat dicari, sehingga di dapat Med = M mod n untuk setiap M < n.
2. Relatif lebih gampang untuk menghitung M^e dan C^d untuk setiap nilai dari M < n.
3. Susah dalam praktek untuk mencari d dengan diberikan e dan n. ed = $k\theta(n) + 1$

Persamaan ini menjadi :

- ed = 1 mod θn)
- $d = \frac{1+k\theta(n)}{e}$

Ringkasan dari algoritma RSA adalah sebagai berikut :

Key Generator

- Pilih p,q p dan q prima, $p \neq q$
- Hitung $n = p * q$
- Hitung $\theta(n) = (p - 1)(q - 1)$
- Pilih *integer* e (θ (n),e) = 1; 1 < e <$\theta(n)$
- Hitung d $d = \frac{1+k\theta\ (n)}{e}$
- *Public-key* KU = {e,n}
- *Private-key* KR = {d,n}

Enkripsi :

- *Plaintext* M < n
- *Ciphertext* $C = M^e \pmod n$

Dekripsi

- *Ciphertext* C
- *Plaintext* $M = C^d \pmod n$

2.3 *Algoritma RSA*

Algoritma RSA ditemukan oleh Ron Rivest, Adi Shamir, dan Len Adleman pada tahun 1977 di *Massachusetts Institute of Technology* (MIT) dan dipublikasikan pada tahun 1978 [4]. RSA menggunakan dua buah bilangan bulat prima untuk mendapatkan *public key* dan *private key* yang akan digunakan dalam proses enkripsi dan dekripsi pesan. RSA digunakan pada aplikasi ini untuk mengenkripsi pesan rahasia yang berupa *file* agar keamanan dari pesan rahasia tadi semakin kuat. Proses dari enkripsi dilakukan sebelum *file* rahasia disembunyikan pada arsip ZIP [5].

Penemuan Clifford Cocks tidak terungkap hingga tahun 1997 dikarenan alasan top-secret classification. Algoritma tersebut dipatenkan oleh *Massachusetts Institute of Technology* pada tahun 1983 di Amerika Serikat sebagai U. S. Patent 4405829. Paten tersebut berlaku hingga 21 September 2000. Semenjak Algoritma RSA dipublikasikan sebagai aplikasi paten, regulasi di sebagian besar negara-negara lain tidak memungkinkan penggunaan paten. Hal ini menyebabkan hasil temuan Clifford Cocks di kenal secara umum, paten di Amerika Serikat tidak dapat mematenkannya [5].

2.4 Keamanan

a. Masalah Kemanan

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Salah satu hal penting dalam komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin keamanan pesan, data atau pun informasi adalah enkripsi. Enkripsi dapat diartikan sebagai sebuah proses yang dilakukan untuk mengubah pesan asli menjadi pesan yang tersandikan. Sebuah *cipher* adalah sebuah algoritma untuk menampilkan enkripsi dan kebalikannya dekripsi. Informasi yang asli disebut sebagai *plaintext*, dan bentuk yang sudah dienkripsi disebut sebagai *ciphertext*. Pesan *ciphertext* berisi seluruh informasi dari pesan *plaintext*, tetapi tidak dalam format yang dapat dibaca oleh manusia ataupun komputer tanpa menggunakan mekanisme yang tepat untuk melakukan dekripsi [1].

b. Aspek-Aspek Keamanan

Keamanan data dan informasi memiliki beberapa aspek penting, antara lain :

1. *Authentification*
2. *Integrity*
3. *Non-repudiation*
4. *Authority*
5. *Confidentiality*
6. *Availability*

Ada 2 metode keamanan data yang digunakan yaitu Kriptografi menggunakan algoritma *Advanced Encryption Standard* (AES) dan Steganografi menggunakan *Command*/DOS.

III. METODE PENELITIAN

3.1 Waktu dan Tempat Penelitian

Waktu Penelitian ini akan dilaksanakan selama satu bulan. Tempat penelitian dan pengumpulan data tidak terikat karena didasarkan dari pengujian.

3.1.1 Metode Pengumpulan Data

Metode pengumpulan data digunakan untuk memperoleh data yang dapat mendukung permasalahan yang akan dibahas. Sehubungan dengan hal ini maka digunakan metode pengumpulan data yang meliputi :

a. Studi Pustaka

Pada metode ini, sebagai tahap awal penulis mencari data.

b. Pengujian Lab

Pada metode ini, penulis melakukan pembuatan aplikasi dengan menggunakan bahasa pemrogaman visual basic, setelah aplikasi berjalan selanjutnya melakukan tahap uji coba langsung terhdap data yang akan di enkripsi dan dekripsi.

3. 2 *Hardware* dan *Software*

3.2.1 *Hardware*

Adapun hardware yang digunakan yaitu dengan spesifikasi sebagai berikut :

1. Laptop *Intel Core* i3
2. *RAM* 2 GB
3. *Hardisk* 500 GB
4. Monitor 14 *inchi* LCD

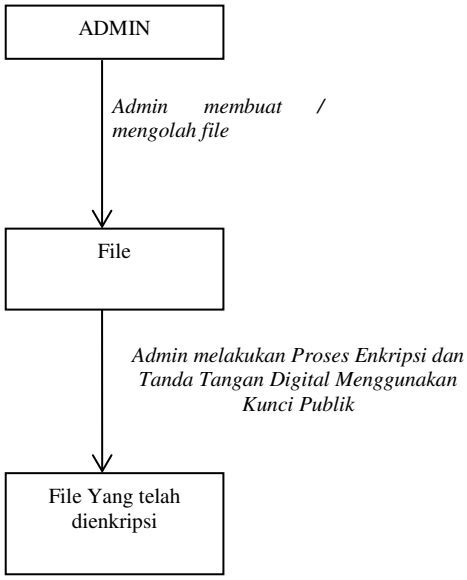
3.2.2 *Software*

Spesifikasi perangkat lunak (*software*) yang dibutuhkan untuk menunjang aktivitas berjalannya sistem dengan baik adalah :

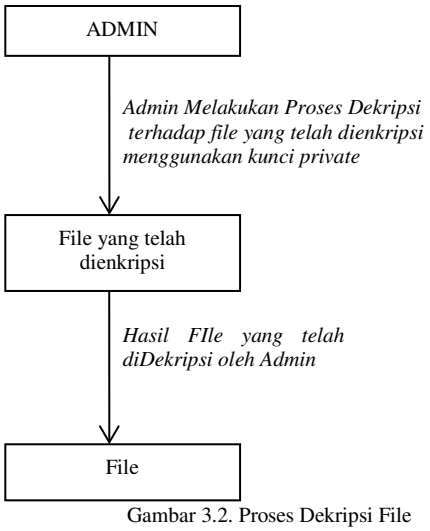
1. Sistem Operasi *Windows* 7
2. Bahasa Pemrogaman *Visual Basic* 6

3.3 Metode Perancangan Sistem

Prosedur sistem ini berguna untuk menunjukkan prosedur penerapan algoritma *RSA* pada suatu *file*. Sistem dimulai dengan melakukan penginstalan aplikasi pada komputer yang digunakan untuk mengolah *file*. Untuk lebih jelasnya proses enkripsi dan dekripsi yang dilakukan oleh admin terhadap sebuah *file,* dapat dilihat pada gambar di bawah ini.



Gambar 3.1. Proses Enkripsi *File*



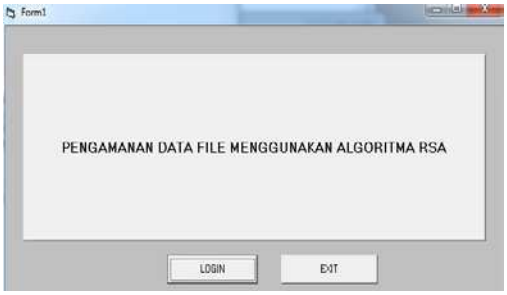
Gambar 3.2. Proses Dekripsi File

IV. HASIL DAN PEMBAHASAN

Setelah proses perancangan, maka tahap selanjutnya adalah tahap implementasi yang dibuat ke dalam bentuk suatu perangkat lunak. Bab ini akan menjelaskan implementasi dari rancangan pada bab sebelumnya.

4.1 Menu Awal

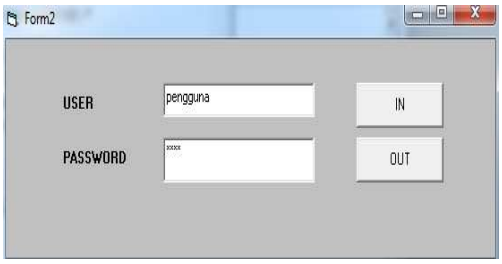
Tampilan dari Menu Awal terdiri dari Dua tombol yaitu tombol *Login* dan *Cancel*. Tombol *Login* akan menampilkan *Form Login*. Sedangkan tombol Cancel akan menyebabkan batal melanjutkna ke form selanjutnya.



Gambar 4.1 Menu Awal

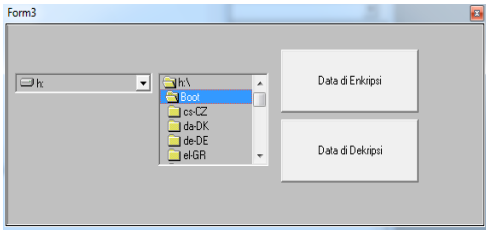
4.1.1 Proses Enkripsi

Pada Form Enkripsi dan Dekripsi, terdapat tampilan Pilih Folder Data, Pilih Data Teks, Hasil dan Pilih Proses.



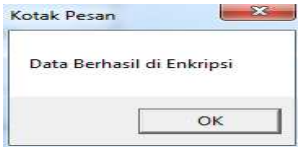
Gambar 4.3 Menu Enkripsi dan Dekripsi

Selanjutnya akan tampil menu enkripsi dan dekripsi data atau *file* :



Gambar 4.4 Menu Enkripsi Data

Setelah Data ditemukan, maka tombol Enkripsi ditekan akan memberikan pemberitahuan nama kunci dari data tersebut seperti pada Gambar 4.5.



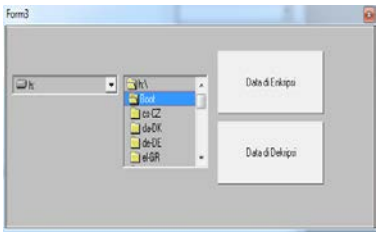
Gambar 4.5 Pesan Proses Enkripsi

4.1.2 Proses Dekripsi

Pada proses Dekripsi hampir Tampilan menu Dekripsi sama dengan proses Enkripsi, telah di Enkripsi dan selanjutnya menekan tombol Dekripsi. Ditunjukkan pada Gambar 4.6.

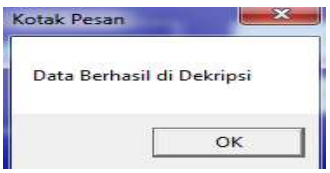
Tabel 1 Form Pada Aplikasi

No	Antarmuka	Sub Antarmuka	Hasil
1	Form Menu Utama	Form Login dan Cancel	Baik
2	Form Login	Form Login	Baik
3	Form Enkripsi dan Dekripsi	Pilih Folder Data	Baik
4	Form Enkripsi dan Dekripsi	Pilih Data Teks	Baik
5	Tombol Enkripsi	Proses Enkripsi	Baik
6	Tombol Dekripsi	Proses Dekripsi	Baik



Gambar 4.6 Proses Dekripsi Data

Selanjutnya akan tampil pesan bahwa Data Sudah di Dekripsi.



Gambar 4.7 Pesan Proses Dekripsi

4.2 Pengujian Sistem

Pengujian adalah proses pemeriksaan atau evaluasi sistem atau komponen sistem secara manual atau otomatis untuk memverifikasi apakah sistem memenuhi kebutuhan-kebutuhan yang dispesifikasikan atau mengidentifikasi perbedaan-perbedaan antara hasil yang diharapkan dengan hasil yang terjadi.

Pengujian yang akan dilakukan pada aplikasi ini adalah pengujian integrasi, pengujian antarmuka dan pengujian kehandalan dengan menggunakan metode *black box testing*.

4.2.1 Pengujian Form Interface

Pengujian form interface merupakan pengujian terhadap sistem atau subsistem lengkap dengan komponen-komponen penyusunnya yang terintegrasi. Metode yang digunakan pada pengujian ini adalah *black box*. Dengan *black box*, pengujian hanya dilakukan pada representasi sistem yang terlihat tanpa perlu mengetahui bagaimana cara kerja sistem tersebut.

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dari pembahasan di atas, maka dapat disimpulkan bahwa :

1. Aplikasi pengamanan data menggunakan algoritma *RSA* mempunyai dua teknik pembacaan yaitu teknik enkripsi (mengubah *file* asli menjadi *file* yang tidak dapat dibaca) dan teknik dekripsi (mengubah *file* yang tidak dapat dibaca menjadi *file* asli).
2. Aplikasi pengamanan mempunyai kalimat sandi / *passphare* yang harus diingat dan bersifat sensitif, maksudnya huruf besar dan kecil dibedakan,agar *passphare* sulit ditebak oleh siapapun.
3. Setelah melakukan uji coba, *file* yang telah diterapkan aplikasi pengamanan akan memiliki empat aspek keamanan, yaitu kerahasiaan, integritas data, otentikasi, dan nir-penyangkalan.

5.2. Saran

Berdasarkan penelitian yang dilakukan maka penulis menyarankan untuk memperhatikan keamanan *file*. Karena bisa saja sewaktu-waktu *file* tersebut dimanipulasi oleh pihak yang tidak berwenang. Penulis menyarankan untuk menerapkan aplikasi pengamaman.

REFERENSI

[1] Andi Riski Alvianto dan Darmaji. *Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android*. Surabaya. 2015.

[2] Megah Mulya. *Perbandingan Kecepatan Algoritma Kriptografi Asimetri*. Palembang. 2013.

[3] Zainal Arifin. *Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman*. Samarinda. 2009.

[4] Fresly Nandar Pabokory, Indah Fitri Astuti, Awang Harsa Kridalaksana. *Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard.* Samarinda. 2015.

[5] Arya Reza Nugraha dan Ary Mazharuddin S, *Penyembunyian Pesan Rahasia yang Terenkripsi Menggunakan Algoritma RSA pada Media Kompresi*. Surabaya. 2013.